

Discovery of Rogue Access Point Location  
in Wireless Network Environments

CROSS-REFERENCE TO RELATED APPLICATIONS

The present application is a continuation-in-part of U.S. Application Ser. No. 10/611,660 filed June 30, 2003 and entitled "Containment of Rogue Systems in Wireless Network Environments."

This application also makes reference to the following commonly owned U.S. patent applications and/or patents, which are incorporated herein by reference in their entirety for all purposes:

U.S. patent application Ser. No. 10/155,938 in the name of Patrice R. Calhoun, Robert B. O'Hara, Jr. and Robert J. Friday, entitled "Method and System for Hierarchical Processing of Protocol Information in a Wireless LAN;" and

U.S. patent application Ser. No. 10/407,357 in the name of Patrice R. Calhoun, Robert B. O'Hara, Jr. and Robert J. Friday, entitled "Method and System for Hierarchical Processing of Protocol Information in a Wireless LAN."

U.S. patent application Ser. No. 10/407,370 in the name of Patrice R. Calhoun, Robert B. O'Hara, Jr. and David A. Frascone, entitled "Wireless Network System Including Integrated Rogue Access Point Detection;" and

U.S. patent application Ser. No. 10/447,735 in the name of Robert B. O'Hara, Jr., Robert J. Friday, Patrice R. Calhoun, and Paul F. Dietrich, entitled "Wireless Network Infrastructure Including Wireless Discovery and Communication Mechanism."

FIELD OF THE INVENTION

The present invention relates to wireless computer networks and, more particularly, to methods, apparatuses and systems directed to the containment of rogue access points and clients in wireless network environments.

## BACKGROUND OF THE INVENTION

Market adoption of wireless LAN (WLAN) technology has exploded, as users from a wide range of backgrounds and vertical industries have brought this  
5 technology into their homes, offices, and increasingly into the public air space. This inflection point has highlighted not only the limitations of earlier-generation systems, but the changing role WLAN technology now plays in people's work and lifestyles, across the globe. Indeed, WLANs are rapidly changing from convenience networks to business-critical networks. Increasingly users are depending on  
10 WLANs to improve the timeliness and productivity of their communications and applications, and in doing so, require greater visibility, security, management, and performance from their network.

As enterprises and other entities increasingly rely on wireless networks, monitoring and management of the components implementing the wireless  
15 network environments becomes critical to performance and security. Indeed, wireless networks pose security risks not generally encountered in wired computer networks. For example, employees or malicious users may connect an unauthorized ("rogue") wireless access point to the corporate network, exposing the network to any wireless client in the coverage area of the access point, and possibly  
20 affecting the performance of the enterprises own wireless network infrastructure.

To detect rogue access points affecting a wireless network deployment, prior art processes, such as site surveys and periodic inspections, typically involve a human tester roaming throughout the wireless network environment with specialized equipment, such as a WLAN tester, that sweeps the wireless coverage  
25 area and stores the resulting data for analysis of one or more attributes of the wireless network deployment, such as the presence and identity of access points. Such site surveys and inspections, however, are time consuming and expensive. In addition, the analysis of the wireless network environment is performed with data gathered at a single point in time and, therefore, is not responsive to periodic or

subsequent changes associated with the wireless network environment (such as installation of new rogue access points, etc.).

In addition, rogue access points may also affect the performance of a wireless network. In an Ethernet LAN (IEEE 802.3), the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol establishes how simultaneous transmissions (packet collisions) are handled. In a WLAN, collision detection in this manner is not possible due to what is known as the "near/far" problem: to detect a collision, a station must be able to transmit and listen at the same time. To account for this difference, the 802.11 protocol uses a slightly different protocol known as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) or the Distributed Coordination Function (DCF). CSMA/CA attempts to avoid packet collisions by using explicit packet acknowledgement (ACK), which means that an ACK packet is sent by the receiving station to confirm that a packet arrived intact. CSMA/CA works by having the transmitting wireless station sense the air for wireless traffic. If there is no activity detected, the transmitting wireless station will wait an additional random period of time. If there still is no activity, the wireless station transmits the data. If the packet is received intact, the receiving station will send an ACK frame that, once received by the original sender, completes the transmission. If the ACK command is not received in a predetermined period of time, the data packet will be resent under the assumption that the original packet experienced a collision. CSMA/CA also handles other interference and radio-wave related problems effectively, but creates considerable overhead. Accordingly, the presence of rogue access points operating on overlapping channels within the vicinity of an authorized access affects the performance of the enterprise's wireless network.

Given the collision avoidance mechanisms employed in 802.11-compliant wireless networks, management and monitoring of the wireless network airspace (for example, to ensure that wireless access points do not interfere with one another) are critical to the performance of the wireless network environment. The

administrative or management functionality associated with WLAN networks, however, generally lacks an integrated and/or automated means of detecting rogue access points. Hand-held scanners, AP startup scans, or full-time scanning devices are the current methods of obtaining data characterizing the network devices  
5 within a wireless network environment. Accordingly, many WLANs do not perform at optimum speed due to overlapping channel interference and rogue access points (i.e., access points installed without authorization and/or knowledge of a network administrator). To address the problems discussed above, U.S. patent application Ser. No. 10/155,938 discloses a wireless network system featuring integrated rogue  
10 access point detection, where access points or elements periodically go off-channel to scan their respective coverage areas for rogue access points.

While this system allows for identification of rogue access points, the system does not provide any mechanism to contain or disable the rogue access points once detected. After being notified of a rogue access point, the network administrator  
15 could attempt to physically locate it based on the known locations of the authorized access point(s) that detected the rogue access point, and then manually disable it. The enterprise or other network, however, is still vulnerable to the security issues discussed above, as well as performance degradation, until the network administrator has the time and ability to locate and disable the rogue access point.  
20 This time lag could prove critical if the rogue access point is employed by a malicious user.

In light of the foregoing, a need in the art exists for methods, apparatuses and systems that facilitate discovery, location, and containment of rogue access points in wireless network environments. A need further exists in the art for  
25 methods directed to the containment of rogue access points that can be automatically implemented. A need further exists for methods of containing rogue access points that utilize the existing wireless network infrastructure. Embodiments of the present invention substantially fulfill these needs.

## SUMMARY OF THE INVENTION

The present invention provides methods, apparatuses and systems facilitating location or containment of rogue or unauthorized access points on wireless computer network environments. Embodiments of the present invention support one to a plurality of rogue containment methodologies. A first rogue containment type involves identification of the physical connection of the rogue access point to the wired network infrastructure and, thus, allows for disabling of that physical connection to contain the rogue access point. Other rogue containment methods involve wireless techniques for containing the effect of rogue access points. In some embodiments, the present invention provides methods, apparatuses and systems facilitating network location of rogue access points to determine whether one or more rogue containment methodologies should be applied.. As discussed below, the rogue location and containment functionality described herein can be applied to a wide variety of wireless network system architectures.

## DESCRIPTION OF THE DRAWINGS

Figure 1 is a functional block diagram illustrating a wireless network system according to an embodiment of the present invention.

Figure 2 is a flow chart diagram providing a method directed to the containment of rogue access points.

Figure 3 is a flow chart diagram showing a method, according to another embodiment of the present invention, directed to the containment of rogue access points.

Figures 4A and 4B are flow chart diagrams illustrating methods for containing rogue access points involving the targeting of wireless clients that associate with rogue access points.

Figure 5 is a functional block diagram illustrating an alternative wireless network system architecture in which the rogue containment functionality can operate.

Figure 6 is a functional block diagram providing yet another wireless network system architecture in which the rogue containment functionality can operate.

Figure 7 is a functional block diagram showing a WLAN system operating in connection with a LAN implemented by a plurality of LAN switches in a hierarchical topology.

Figure 8 is a functional block diagram illustrating the process flow associated with an embodiment of the rogue location discovery methodology of the present invention.

Figure 9 is a flow chart setting forth a method, according to an embodiment of the present invention, directed to discovering the logical network location of a detected rogue access point.

#### DESCRIPTION OF PREFERRED EMBODIMENT(S)

The rogue containment functionality described herein assumes that one or more rogue access points have been detected. U.S. application Ser. No. 10/155,938, identified above, discloses methods, apparatuses and systems for detecting rogue access points over the airspace associated with a wireless network environment. However, the method according to which rogue access points are detected, as well as the devices and systems employed to detect them, are not critical to the rogue containment functionality of the present invention. Rogue access point detection may, as described in the above-identified application, be integrated into the wireless network environment and, therefore, automated. Alternatively, rogue access point detection may be executed in a more manual fashion, such as manually sweeping different coverage areas with a WLAN tester. However, as disclosed in U.S. application Ser. No. 10/155,938, the wireless network system can,

in one embodiment, report detected rogue access points to a network administrator. The network administrator then has the option of placing the detected access point on an ignore list, or otherwise taking no action as to the rogue access point. Alternatively, the network administrator may initiate one or more rogue  
5 containment operations as described more fully below. In other embodiments, the rogue containment functionality may also be integrated into the wireless network system and may be automatically triggered upon detection of one or more rogue access points. The rogue containment functionality described herein may be physically integrated into the devices that implement a wireless network system,  
10 or may be embodied in dedicated, specialized network equipment. For example, the rogue containment functionality according to embodiments of the present invention may be embodied in a central rogue containment device 21 (see Figure 6). In another embodiment, the rogue containment functionality may be embodied in one or more central control elements 24, 26 in a wireless network system featuring  
15 hierarchical processing of protocol information (see Figure 1).

As discussed in more detail below, embodiments of the present invention support one to a plurality of rogue containment methodologies. A first rogue containment type involves identification of the physical connection of the rogue access point to the wired network infrastructure and, optionally, the disabling of  
20 that physical connection to contain the rogue access point. Other rogue containment methods involve wireless techniques for containing rogue access points.

#### A. Rogue Traffic Containment using Wired Network Infrastructure

25 Figure 2 illustrates the process flow, according to an embodiment of the present invention, directed to containing detected rogue access points using wired network or LAN-based functionality. For didactic purposes, the rogue containment functionality is integrated into a rogue containment device 21 in the wireless network system of Figure 6. In one embodiment, rogue containment device 21 is a

server or other computing platform configured to execute the rogue containment functionality described herein. In such an embodiment, the rogue containment device 21 includes a network interface allowing for communication of data between it and access elements 112, 114, and 116, as well as a rogue containment module  
5 operative to execute the functionality described herein. As discussed below, rogue containment device 21 operates in connection with one or more access points 112, 114, 116. However, rogue containment device 21 may operate with radio transmit/receive units dedicated to rogue containment and spaced throughout the wireless network environment.

10 As Figure 2 illustrates, detection of a rogue access point, in one embodiment, triggers or initiates the process described herein (102). As to a detected rogue access point, rogue containment device 21 identifies the MAC address of at least one rogue wireless station that has associated with the detected rogue access point (104). U.S. Application Ser. No. 10/155,938 discloses monitoring for packets on a  
15 given channel and recording information about the packets in a data structure. Upon detection of a rogue access point, certain information concerning the rogue access point is available, such as the wireless MAC address of the rogue access point. Other information may also potentially be available. For example, certain 802.11 frames, such as data frames, may also include the MAC address of a client  
20 wireless station. Certain 802.11 frames also include the Service Set Identifier (SSID) associated with the access point or element, such as beacon frames, probe responses and association requests, as well as its operating channel. If the initial scan for rogue access points yielded the MAC address for at least one wireless client associated with the rogue access point, then rogue containment device 21 can  
25 use this MAC address. However, if no wireless client MAC address is obtained from the initial rogue scan data, rogue containment device 21 can direct one or more access points (e.g., access points 114, 116) that originally detected the rogue access point to operate in a scan mode to identify data frames or other frames sourced from a wireless client and transmitted to the detected rogue access point.



In one embodiment, the channels on which the scan is performed can be limited to the channel(s) detected in the initial scan or on a subset of channels centered around the channels advertised by the rogue access point (as in beacon frames), or the channels on which rogue traffic was originally detected by one or more access  
5 points. In another embodiment, the scan can be performed on all available frequency channels. One of ordinary skill in the art with knowledge of the wireless protocol employed will recognize how to obtain the requisite information. In 802.11 networks, the frames include a control field allowing for resolution of the frame type and the direction of the packet (e.g., from or to an access point).

10 With knowledge of one or more wireless client MAC addresses, rogue containment device 21 then transmits SNMP queries to the network devices implementing LAN 10 or WAN 50 (e.g., switches, hubs, bridges, etc.) to identify which network devices have encountered packets sourced from the wireless client(s). As discussed above, an access point typically bridges wireless traffic  
15 between wireless clients and the wired network to which the access point is connected. Pursuant to this bridging operation, the wireless 802.11 headers are stripped from the packets and replaced with the appropriate layer 2 protocol header, such as 802.3 (Ethernet). The source MAC address in the 802.3 header is the MAC address of the source wireless station. Still further, networking  
20 equipment, such as a LAN switch, maintains the source MAC addresses of packets encountered on a given port of the device in a management information base (MIB), which can be polled via SNMP queries. In one embodiment, rogue containment device 21 polls all devices with SNMP queries using one or more wireless station MAC addresses to identify the network device(s) that has(have) encountered a  
25 packet sourced from the identified rogue wireless client(s) (108). Rogue containment device 21 then polls the responding network device(s), again using SNMP queries, for the port of the network device that encountered the source wireless MAC address (110).

If there is no affirmative response to the SNMP queries, it can be assumed that the detected rogue access point is connected to another network, such as a network associated with a neighboring enterprise located, for example, in another room, building or floor. Alternatively, it can be assumed that the detected rogue  
5 access point is also operating as a Network Address Translation (NAT) device. In this instance, the SNMP queries can use the wireless MAC address of the rogue access point, as the wireless and wired MAC addresses are sometimes identical. In the circumstances where no SNMP response is returned, rogue containment device  
21 can simply report the detected rogue access point to a network administrator, or  
10 implement the rogue location discovery methodology described more fully below.

In layered LAN topologies, such as a plurality of LAN switches arranged in a hierarchical configuration (see Figure 7), more than one network device may respond. Specifically, Figure 7 sets forth a network implemented by a plurality of LAN switches 23a, 23b, 23c, 23d and 23e. Packets sourced from a rogue wireless  
15 client and bridged by rogue access point 99 (destined for computer network 50 via router 97 and access link 96, for example) may be encountered by switches 23a and 23b. In these network configurations, rogue containment device 21 attempts to identify the network device to which the rogue access point 99 is directly connected. This allows only the port on switch 23b to which the rogue access point 99 is  
20 connected to be disabled without affecting other network traffic.

The IEEE 802.1d specification describes the spanning tree protocol and the methods according to which LAN switches keep track of or report MAC addresses encountered on each port. Using standard methodologies disclosed in the 802.1d specification, rogue containment device 21 can ascertain the LAN switch and port  
25 to which the rogue access point 99 is directly connected by querying, via SNMP, the 802.1d (spanning tree) tables maintained in the management information base (MIB) of the switches 23a-e implementing the network. Generally speaking, however, the switch with the least number of MAC addresses on a port associated

with the rogue access point MAC address is usually the switch to which the rogue access point is directly connected.

Rogue containment device 21 can report this information to a network administrator, via an email or other suitable message to allow the network administrator to manually configure the appropriate LAN switch (switch 23b in the example) or other network device to disable that port. Alternatively, the network administrator can physically disconnect the rogue access point 99 from the identified port. In the embodiment shown in Figure 2, however, rogue containment device 21 can automatically transmit an SNMP query to the appropriate network device to disable the port to which the rogue access point is connected (112).

In one embodiment, the rogue containment device 21 (or other device containing the rogue containment functionality described herein) is configured with knowledge of the IP addresses of each LAN switch 23a-e or other network device, the SNMP read community name, and optionally the SNMP write community name (to allow rogue containment device to disable the port to which the rogue access point is connected).

## B. Wireless Containment Functionality

As discussed above, wireless mechanisms and methods for containing rogue access points are also possible in addition to or in lieu of the wired network approach discussed above. In certain embodiments, the rogue containment functionality of the present invention takes advantage of the behavior of 802.11 wireless systems as it relates to the network allocation vector to contain rogue access points. In other embodiments, the rogue containment functionality targets the wireless stations that associate with the rogue access points and forces them to terminate their respective connections to the rogue access point.

### B.1. Using Network Allocation Vector

802.11 wireless networks feature a virtual carrier-sense mechanism that facilitates the sharing of the wireless medium among a plurality of wireless stations. The virtual carrier-sense mechanism is achieved by distributing reservation information announcing the impending use of the medium by a given wireless station. The exchange of Request-to-Send (RTS) and Clear-to-Send (CTS) frames prior to transmission of the actual data frame is one means of distribution of this reservation information. The RTS and CTS frames contain a Duration/ID field that defines the period of time that the medium is to be reserved to transmit the actual data frame and the returning ACK frame. As to the duration value used, the wireless transmitter calculates a duration value corresponding to (based on) a set of rules defined by the 802.11 protocol. All wireless stations within the reception range of either the originating station (which transmits the RTS) or the destination station (which transmits the CTS) learn of the medium reservation. All wireless stations also use the Duration/ID field in data frames to identify the medium reservation as well.

The network allocation vector (NAV) is an indicator, maintained by each wireless station, of time periods when transmission onto the wireless medium will not be initiated by the station whether or not the station's clear channel assessment (CCA) function senses that the wireless medium is busy. All stations process Duration field values less than or equal to 32,767 from valid data frames to update their NAV settings as appropriate under the coordination rules defined in the 802.11 specification. The NAV is essentially a counter, which counts down to zero at a uniform rate. When the NAV counter is zero, the virtual carrier-sense indication is that the medium is idle; when nonzero, the indication is busy. As each station receives medium reservation information in the frames transmitted over the wireless medium, the NAV is reset and begins counting down.

An embodiment of the present invention takes advantage of the virtual carrier-sense mechanism to contain the effect of rogue access points. As Figure 3 illustrates, when a rogue access point is detected (202), rogue detection device 21

identifies the authorized access points that neighbor the detected rogue access point (204). In one embodiment, this determination is made by assessing which access points detected frames transmitted to/from the rogue access point 99. In another embodiment, the determination may further be made based on location  
5 information of the authorized access points. After identification of neighboring access points, rogue detection device 21 selects one or more access points for rogue containment (206). Rogue containment device 21, in one embodiment, makes this selection based on the observed signal strength of frames sourced by the rogue access point 99. Rogue containment device 21 then configures the selected  
10 neighboring access point(s) to contain the rogue access point 99 (208).

In one embodiment, rogue containment exploiting the virtual carrier-sense mechanism is intended to disable all wireless traffic (authorized or unauthorized) in the approximate vicinity of the rogue access point 99. In such an embodiment, the selected access points are configured to transmit data frames intended to block  
15 wireless traffic on all available frequency channels. In one embodiment, the duration value in each frame is set to the maximum value allowed by the 802.11 or other applicable networking protocol. In one embodiment, the destination address of the data frame is set to a randomly-chosen or arbitrary value. The repetition interval for transmitting the data frames on each channel is less than the duration  
20 specified in the data frames. Accordingly, the maximum duration value need not be used as long as the repetition interval between data frames is less than the duration value. Since the virtual carrier-sense mechanism is not specific to a given Basis Service Set or BSSID, the repetition of data frames on all available channels causes all access points (authorized and rogue) that detect the data frames to reset  
25 their respective NAV counters, and continue to reset them before the counters approach zero, which would allow for transmission of frames. In this manner, all access points and wireless stations within range are effectively disabled during the time the selected access point(s) operate in this rogue containment mode.

In another embodiment, the rogue-containing data frames can be transmitted on selected channels to permit, if possible, authorized access points to operate within the vicinity of the rogue access point. In one embodiment, the access points that scan for rogue access points can also report the channels on which rogue traffic was detected. Channel information is also available from Beacon and Probe Response frames in 802.11 network environments. Rogue containment device 21 can use this channel information to select channels on which to transmit the rogue containing frames. For example, if a rogue access point is detected as operating on channel 5 in an 802.11b wireless network, rogue containment device 21 can configure one or more access points to transmit rogue containing frames on that channel or on a range of channels (e.g., 4 to 6) centered on channel 5. Use of selected channels, as opposed to all channels, requires additional monitoring in the event that the rogue access point changes its operating channel. In addition, rogue containment device 21 may also configure neighboring access points to operate on different, non-overlapping channels from the detected rogue access point(s), if possible. Use of selected channels also allows the access point(s) transmitting rogue containing frames to switch between a normal access point mode (serving authorized wireless stations) and a rogue containment mode (periodically going off channel to transmit rogue-containing data frames). In one embodiment, the transmission of rogue-containing frames, in addition to the timing considerations discussed above, is coordinated with the data link layer functionality of the access point. U.S. Application Ser. No. 10/447,735 discloses coordinating transmission of frames with data link layer functionality to avoid interrupting the transmission of beacon frames. This method can be adapted to coordinate transmission of rogue containing frames with transmission of beacon frames.

## B.2. Targeting Rogue Clients

As discussed above, the rogue containment functionality, according to an embodiment of the present invention, targets wireless clients that have authenticated and/or associated with rogue access points. In one embodiment, and as Figures 4A and 4B illustrate, detected rogue access points are added to a containment list. In one embodiment, a separate process spoofs the rogue access points and transmits deauthentication frames, causing the wireless stations that have associated with the rogue access point to terminate their connections.

In a specific embodiment, when wireless traffic from a rogue access point is detected (302), rogue containment device 21 determines whether the traffic corresponds to a new rogue access point (304). If so, rogue containment device determines the attributes of the rogue access point (e.g., MAC address, BSSID, transmission channel, etc.) (308) and adds the newly detected rogue access point to a containment list (310). The transmission channel can be determined, as discussed above, by examining certain frames, such as Beacon or Probe Response Frames, or by the channel on which rogue traffic was detected. In one embodiment, rogue containment device 21 stores the operating channel in association with the detected rogue access point on the containment list. In one embodiment, the containment list is implemented in a table or other data structure and includes the following fields: 1) MAC address (primary key), 2) BSSID, and operating channel. In one embodiment, the fields also contain the last N (e.g., 3) operating channels for each known rogue access point. In one embodiment, the containment list also includes identifiers corresponding to the authorized access points that detected the rogue access point during respective rogue AP scans. If the detected rogue traffic involves a known rogue access point (i.e., an access point previously detected during a scan), rogue containment device 21 re-determines the attributes of the rogue access point (308) and modifies the corresponding entry in the containment table (310). In one embodiment, if a new operating channel is detected, the last N channels field and the current channel field are updated

accordingly. If the rogue access point has been physically moved to another location, this change can also be detected by comparing the access points that currently detect the rogue access point with the access points that previously detected the rogue. As Figure 4A illustrates, rogue containment device 21 then  
5 selects and configures the access point(s) that will be used to target clients of the rogue access point (312). The selection can be based on the access points that detected the rogue access point, as well as other factors such as the signal strength detected by the access points, geographic proximity of other access points, operational load, and the like. In one embodiment, rogue containment device 21  
10 configures the selected access points with a subset of the containment list including the rogue access points which the selected access points have been selected to contain.

In one embodiment, the selected authorized access points can be configured to periodically transmit deauthentication frames at fixed repetition intervals. The  
15 repetition interval, in one embodiment, is a heuristically determined value that is sufficient to prevent meaningful access to wireless clients of a detected rogue access point. In one embodiment, the repetition interval is a fixed value. However, in the embodiment described below, the repetition interval can be adjusted in response to detected wireless traffic associated with rogue clients. In one embodiment, the  
20 repetition interval is 100 ms; however, the repetition interval will depend on the particular wireless network environment and the time it takes for wireless clients to authenticate and associate with access points. The deauthentication frames are transmitted, in one embodiment, using the broadcast address as the destination address.

25 Figure 4B illustrates a method, according to an embodiment of the present invention, executed by an access point that has been configured to target clients of a detected rogue access point. As discussed above, the access point spoofs the rogue access point (i.e., transmits frames using the MAC address and BSSID of the rogue access point), and periodically transmits deauthentication frames causing clients of



the rogue access point to terminate their connections. As Figure 4B shows, the repetition interval (R) is initially set to a first value, such as 100 milliseconds, (320) and decreased (328) if wireless traffic associated with the rogue clients are detected in subsequent scans, such as data frames, ACK frames, etc. transmitted from or to the wireless stations (326). Certain detected wireless traffic from the rogue access point itself, such as Beacon Frames, does not decrease the repetition interval, since Beacon Frames are periodically transmitted without regard to the state or activity of the clients. Similarly, other wireless frames sourced from clients, in one embodiment, would not decrease the repetition interval, such as authentication and association request frames.

As Figure 4B illustrates, when it is time to transmit deauthentication frames (324), the access point retrieves the rogue access point data (MAC address and BSSID) (330). In one embodiment, for each rogue access point on the containment list (332), the access point transmits deauthentication frames on all available operating channels (334, 336). This process is repeated at every repetition interval. As discussed above, if wireless traffic from a wireless station that has associated with the rogue client is detected (either by that access point or by other access points during a rogue scan), the repetition interval is decreased (328).

Other variations are possible. For example, the analysis determining whether the repetition interval should be decreased can be performed centrally by the rogue containment device 21 and be applied on a per-access-point basis or, globally, to all access points. In such an embodiment, the rogue containment device 21 receives rogue scan data from access points as described in U.S. application ser. no. 10/155,938 and analyzes the scan data to determine whether any wireless clients have gained access to the network through a known rogue access point. In addition, the channel information contained in Beacon or Probe Response frames or as detected during rogue scans, can be used to narrow the channels on which deauthentication frames are transmitted. In addition, the deauthentication frames

may be transmitted on the last N observed channels for each rogue access point. In addition, rogue detection device 21 can respond in other ways to detecting wireless traffic associated with rogue clients, such as selecting additional or alternative neighboring access points to perform the rogue containment functionality described  
5 herein. In another embodiment, 802.11 disassociation frames can be transmitted in addition to, or in lieu of, deauthentication frames. In one embodiment, the central control element 24 may include a table of known devices identified by OUI (organizational unique identifier) that details the rogue clients that are susceptible to broadcast and/or unicast deauthentication and/or disassociation frames. In such  
10 an embodiment, central control element 24 can determine, based on the OUI table, the optimal way to terminate the connections between the rogue access point and its rogue clients. For example, the central control element 24 may unicast deauthentication frames to individually targeted rogue clients. The OUI table may be populated based on a heuristic evaluation of the known client devices for a  
15 plurality of manufacturers and the observed responses to a variety of deauthentication and/or disassociation frames, repetition intervals, and transmission types (e.g., broadcast or unicast).

In yet another embodiment, rogue containment device 21 configures one or more access points to spoof a detected rogue access point and transmit beacon  
20 packets announcing a Contention-Free Period for an arbitrarily large time value, such as 200 milliseconds. As discussed above, to spoof the rogue access point, the selected access points use the MAC address and BSSID of the rogue access point as the source address in the beacon packets. As above, the beacon packets are transmitted at a repetition interval shorter than the announced contention-free  
25 period to essentially prevent wireless clients from accessing the rogue access points. In one embodiment, the transmission of these beacon packets can be coordinated with the transmission of regular beacon packets using the methods described in U.S. application Ser. No. 10/447,735.

### C. Exemplary Operating Environments

Figures 1, 5 and 6 illustrate exemplary wireless network systems into which the rogue containment functionality can be integrated. The rogue containment functionality described above was described, for didactic, purposes as operating in connection with the wireless network environment of Figure 6. According to the embodiment of Figure 6, access points 112, 114, and 116, in one embodiment, are configured to periodically scan for rogue access points and provide the data obtained during the scan to rogue containment device 21, which then applies one to all of the rogue containment mechanisms discussed above (such as configuring one or more access points 112, 114, 116 to transmit rogue-containing data frames).

As discussed below, however, the rogue containment functionality according to the present invention may be applied to other wireless network architectures. For example, the rogue containment functionality described herein may be integrated into a WLAN environment as disclosed in U.S. application Ser. Nos. 10/155,938 and 10/407,357 incorporated by reference herein. Figure 1 illustrates a wireless computer network environment according to an embodiment of the present invention. Referring to Figure 1, there is shown a block diagram of a wireless Local Area Network system 10 according to an embodiment of the invention. A specific embodiment of the invention includes the following elements: access elements 12, 14 for wireless communication with selected client remote elements 16, 18, 20, 22, central control elements 24, 25, 26, and means for communication between the access elements and the central control elements, typically direct line access 28, 30, but potentially a wireless backbone, fiber or other reliable link. As disclosed in U.S. patent application Ser. No. 10/407,357, in another embodiment, the access elements, such as access elements 12, 14 are directly connected to LAN 10 or a virtual local area network (VLAN) for communication with a corresponding central control element 24, 26. See Figure 5.

The access elements 12-15 are coupled via communication means using a wireless local area network (WLAN) protocol (e.g., IEEE 802.11a or 802.11b, etc.) to

the client remote elements 16, 18, 20, 22. The communications means 28, 30 between the access elements 12, 14 and the central control element 24 is typically an Ethernet network, but it could be anything else which is appropriate to the environment. As described in U.S. Application Ser. No. 10/155,938, the access  
5 elements 12, 14 and the central control element 24 tunnel network traffic associated with corresponding remote client elements 16, 18; 20, 22 via direct access lines 28 and 30, respectively. Central control element 24 is also operative to bridge the network traffic between the remote client elements 16, 18; 20, 22 transmitted through the tunnel with corresponding access elements 12, 14.

10 In one embodiment, the access elements, such as access elements 12, 14, include functionality allowing for detection of the strength of the signal received from client remote elements and/or other access elements. For example, the IEEE 802.11 standard defines a mechanism by which RF energy is measured by the circuitry (e.g., chip set) on a wireless network adapter or interface card. The 802.11  
15 protocol specifies an optional parameter, the receive signal strength indicator (RSSI). This parameter is a measure by the PHY layer of the energy observed at the antenna used to receive the current packet or frame. RSSI is measured between the beginning of the start frame delimiter (SFD) and the end of the PLCP header error check (HEC). This numeric value is typically an integer with an  
20 allowable range of 0-255 (a 1-byte value). Typically, 802.11 chip set vendors have chosen not to actually measure 256 different signal levels. Accordingly, each vendor's 802.11-compliant adapter has a specific maximum RSSI value ("RSSI\_Max"). Therefore, the RF energy level reported by a particular vendor's wireless network adapter will range between 0 and RSSI\_Max. Resolving a given  
25 RSSI value reported by a given vendor's chip set to an actual power value (dBm) can be accomplished by reference to a conversion table. In addition, some wireless networking chip sets actually report received signal strength in dBm units, rather than or in addition to RSSI. Other attributes of the signal can also be used in combination with received signal strength or as an alternative. Again, many chip

sets include functionality and corresponding APIs to allow for a determination of SNRs associated with packets received from client remote elements. In one embodiment, access elements 12, 14 include the detected signal strength and/or SNR value associated with a packet the encapsulating headers used to tunnel the  
5 wireless packets to central control element 24.

As described in the above-identified patent application, central control element 24 operates to perform data link layer management functions, such as authentication and association on behalf of access elements 12, 14. For example, the central control element 24 provides processing to dynamically configure a  
10 wireless Local Area Network of a system according to the invention while the access elements 12, 14 provide the acknowledgment of communications with the client remote elements 16, 18, 20, 22. The central control element 24 may for example process the wireless LAN management messages passed on from the client remote elements 16, 18; 20, 22 via the access elements 12, 14, such as  
15 authentication requests and authorization requests, whereas the access elements 12, 14 provide immediate acknowledgment of the communication of those messages without conventional processing thereof. Similarly, the central control element 24 may for example process physical layer information. Still further, the central control element 24 may for example process information collected at the access  
20 elements 12, 14 on channel characteristic, propagation, and interference or noise. Central control elements 25, 26 and associated access elements 13, 15 operate in a similar or identical manner. Other system architectures are possible. For example, U.S. Application Ser. No. 10/407,357 discloses a system architecture where the access elements, such as access elements 12-15, are directly connected to  
25 LAN segment 10.

As described in U.S. Application Ser. No. 10/407,370, the access elements feature a scanning mode, according to which the access elements monitor their respective coverage areas for wireless traffic relative to at least one frequency channel and gather scan data characterizing detected wireless traffic. The scan

data can be transmitted to a central management device, such as central management platform or a central control element 24 (Figures 1 or 5) for processing and detection of rogue access points. In one embodiment, the access elements operate in a normal access point mode bridging wireless traffic between  
5 WAN 50 and the remote client elements. However, at a regular scanning interval, the access element switches to a scanning mode according to which it monitors its coverage area for wireless traffic for a scanning period.

In one embodiment, the functionality of rogue containment device 21 can be integrated into one or more central control elements 24, 26. In one embodiment,  
10 one of the central control elements 24, 26 is configured as a master central control element to centrally process rogue scan data and make the selection and configuration decisions associated with the rogue containment functionality discussed above for the entire wireless network system. In another embodiment, each central control element 24, 26 can operate in an independent or autonomous  
15 manner with respect to the access elements under its respective control.

#### D. Discovery of Rogue Access Point Location

In one embodiment, the rogue containment functionality causes one or more access elements to associate with a detected rogue access point 99, and transmit  
20 packets to a managed network device for the purpose of determining whether the detected rogue access point is connected to the same network as the managed network devices, such as central control element 24 and access elements 12, 14, as discussed more fully below. This network location information can be used to determine the suitability of one or more of the rogue containment methodologies  
25 described above.

Figure 8 is a functional block diagram illustrating the process flow associated with an embodiment of the rogue location discovery methodology of the present invention. Of course, the rogue location discovery functionality described herein can be implemented in connection with the other wireless LAN

architectures and systems discussed above. Figure 9 is a flow chart setting forth a method, according to an embodiment of the present invention, directed to discovering the logical network location of a detected rogue access point. As Figure 9 illustrates, when a rogue access point is detected (402), central control element 24 identifies the authorized access points (e.g., access points 12, 14) that neighbor the detected rogue access point 99 (204). In one embodiment, this determination is made by assessing which access elements detected frames transmitted to/from the rogue access point 99. In another embodiment, the determination may further be made based on location information associated with the authorized access points.

After identification of neighboring access elements, central control element 24 selects one or more access points to be used to discover the network location of the rogue access point 99 (406). Central control element 24, in one embodiment, makes this selection based on the observed signal strength of frames sourced from the rogue access point 99, as detected by the access elements. Alternatively, or in addition to signal strength, central control element 24 can also select one or more access elements based on their current load, opting to use the access element(s) with lower current load. Once selected, central control element 24, behaving like a wireless client device via a selected access element (e.g. access element 14), attempts to establish a wireless connection to the detected rogue access element 99 (408). In 802.11 environments, using information in the wireless frames that originally led to detection of the rogue access point 99, central control element 24 transmits an authentication request using the MAC address of the rogue access point to rogue access point 99 via access element 14 ((see Figure 8, #1a, 1b). If the rogue access point 99 is configured to use open system authentication, the rogue access point 99 responds with an authentication frame as a response usually indicating an acceptance. As Figure 8 illustrates, access element 14 receives the response and transmits it to central control element 24. If the rogue access point 99 is configured to use shared key authentication, the access point responds with an authentication frame containing challenge text. In this circumstance, central

control element 24 determines that it cannot successfully establish a connection to the rogue access point 99 (410), since it does not have knowledge of the correct WEP key (which is the basis for authentication), which it must use to encrypt the challenge text in an authentication response. In one embodiment, central control  
5 element 24 reports the detected rogue access point 99 to a network administrator, providing detail information such as MAC address, and the like. In another embodiment, central control element 24 may alternatively employ the rogue location and containment functionality discussed in Section A, *supra*, if it is unable to establish a wireless connection to the detected rogue access point 99. In any  
10 event, assuming that the authentication exchange is successful, central control element 24 then transmits an association request to the rogue access point 99 via access element 14, and receives an authentication response (Figure 8, # 1a, 1b).

After a connection is established, central control element 24 via access element 14, in one embodiment, obtains an IP address from the network  
15 infrastructure supported by network 50 (412) (see Figure 8, # 2a, 2b, 2c). For example and in one embodiment, most enterprise network infrastructures support the Dynamic Host Configuration Protocol (DHCP), which provides a method for dynamically assigning IP addresses and configuration parameters to other IP hosts or clients in an IP network. In such an embodiment, access element 14, under  
20 control of central control element 24, transmits a DHCPDISCOVER packet which is broadcast over network 50, which are ultimately transmitted via BootP relay agents to one or more DHCP servers. The DHCP servers respond with a DHCP OFFER packet that includes an available IP address. Central control element 24, acting as a DHCP client, chooses a target server, and broadcasts a  
25 DHCPREQUEST packet indicating its selection and allowing other DHCP servers to release the IP address previously reserved for the client. Of course, other dynamic IP address assignment protocols, such as BootP, can also be used. In another embodiment, central control element 24 can be configured with a suitable IP address to be used in the network environment in which it is deployed. If the



DHCP/IP address obtained indicates that the central control element 24 and the rogue access point are on separate subnets, central control element 24 obtains the MAC address of the gateway router 52, if any, associated with the subnet to which the rogue access point 99 is connected (413). In one embodiment, central control  
5 element 24 via access element 14 issues an ARP request using the IP address of the default gateway found in an option field in the DHCPOFFER packets. The ARP reply contains the MAC address of the port of the gateway router 52 to which the rogue access point 99 is connected (and, therefore, the MAC address to which the rogue location discovery packets must be directed, see below). The same  
10 methodology is also used in circumstances where the rogue access point 99 acts as a NAT/DHCP device, which returns a DHCP address and responds to the ARP request.

As Figure 9 illustrates, central control element 24 then composes and transmits a Rogue Location Discovery (RLD) packet to determine whether the  
15 detected rogue access point 99 is connected to the network 50. Reference arrows 3a, 3b and 3c illustrate the logical path taken by the RLD packet (according to an embodiment), assuming the detected rogue access point 99 is connected to network 50. In one embodiment, the RLD packet is a UDP packet with a IP source address set to the dynamically assigned DHCP address (above), and a destination address  
20 set to the IP address associated with the LAN interface of central control element 24. In another embodiment, the destination address in the RLD packet can be set to the IP address associated with another authorized network device, such as a central management platform, which can communicate receipt of the RLD packet to central control element 24. Of course, the UDP/IP packet is further  
25 encapsulated into a wireless 802.11 data frame for transmission to rogue access point 99, which decapsulates the 802.11 frame and adds a suitable 802.3 header to bridge the frame onto the network 50. In one embodiment, the source address in the 802.11 frame is the MAC address of the access element 14, while the destination address is set to the MAC address either 1) of the central control

element 24 (if it is on the same subnet as the rogue), or 2) that returned in the ARP reply. In one embodiment, the body of the RLD packet includes a digitally signed nonce to allow central control element 24 to verify its authenticity. The RLD packet is then routed and/or switched within network 50 to the LAN interface of central control element 24. Using this mechanism, central control element 24 can readily determine whether the detected rogue access point 99 is connected to the same network 50. In one embodiment, central control element 24 transmits an RLD packet and waits for a response (416). If a response is not received within a threshold period of time, central control element 24, in one embodiment, repeats this process up to a predetermined number of times. If all attempts time out, central control element 24 deems that the rogue access point 99 is not part of the same network 50 and reports the detected rogue access point to a network administrator (420). For example, the detected rogue access point 99 may be associated with an enterprise in a neighboring room, building or floor. However, if central control element 24 receives the RLD packet on its LAN interface (416), central control element 24, in one embodiment, can then operate to report the rogue access point 99 and contain it (418), using one or a combination of the rogue containment functionalities discussed above.

Another embodiment of the present invention does not rely on DHCP server functionality. Rather, by observing the IP addresses (included in the IP headers of the encapsulating 802.11 frames) of wireless clients that are associated with the rogue access point 99, central control element 24 may select one of the observed IP addresses and use the selected IP address as the source address for the RLD packets. The logical network address of the wireless client may be resolved by inspecting the From/To DS bits in the 802.11 frame as well as the source and destination addresses contained in the IP header. This may be used in lieu of obtaining a dynamic IP address from a DHCP server, or in a situation where IP addresses are statically assigned. The MAC address of the default gateway on the subnet can be obtained by inspecting packets and identifying the MAC address that

appears in the MAC source address field of IP packets from many different IP source addresses.

The invention has been explained with reference to specific embodiments.  
5 Other embodiments will be evident to those of ordinary skill in the art. For example, the present invention can also be applied to WLAN architectures employing other wireless protocols beyond the IEEE 802.11 standard. It is, therefore, intended that the claims set forth below not be limited to the embodiments described above.

10